



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,363	01/26/2001	Brant L. Candalore	80398.P213	6441

7590 01/25/2005

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP  
Seventh Floor  
12400 Wilshire Boulevard  
Los Angeles, CA 90025-1026

EXAMINER
----------

KLIMACH, PAULA W

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 01/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application N .

09/771,363

Applicant(s)

CANDELORE, BRANT L.

Examiner

Paula W Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 20 August 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 4-14, 16, 18-22, 24, 26, 28 and 30-33 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 4-14, 16, 18-22, 24, 26, 28, and 30-33 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- 1) ☐ Certified copies of the priority documents have been received.
  - 2) ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - 3) ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Response to Amendment***

This office action is in response to amendment filed on 08/20/2004. Original application contained Claims 1-33. Applicant cancelled Claims 1-3, 15, 17, 23, 25, 27, and 29, and amended Claims 4, 6-7, 9-10, 12, 14, 16, 18-19, 21, 24, 26, 28, and 30-32. The amendment filed on 08/20/2004 have been entered and made of record. Therefore, presently pending claims are 4-14, 16, 18-22, 24, 26, 28, and 30-33.

### ***Response to Arguments***

Applicant's arguments filed 08/20/2004 have been fully considered but they are not persuasive because of the reasons listed in the office action below.

The Applicant argued, "Wasilewski does not teach or suggest key insertion and in fact can be considered to teach away from the claimed invention. Hash functions are not used to insert and subsequently retrieve the inserted data. Hash functions are not used to insert and subsequently retrieve the inserted data. Hash functions destroy the inserted information and produce a hash result, normally a 128-bit value, which is commonly used for comparison with another hash result." This is not found persuasive. Wasilewski discloses a system wherein the key is contained, and therefore, inserted into the EMM (page 4 paragraph 0070). The hash function disclosed by the applicant (page 5 paragraph 0074) is used to contain data used to ensure that the information in the EMM has been transmitted correctly and therefore not been tampered with (page 5 paragraph 0075). This information, sealed digest, and the EMM are sent to the client (page 5 paragraph 0076). Therefore the key is sent to the client without being destroyed.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**Claims 4-14, 16, 18-22, 24, 26, 28, and 30-33** are rejected under 35 U.S.C. 103(a) as being unpatentable over Son in view of Wasilewski (US 20040003008A1).

*In reference to claims 4, 10, 21, and 32* Son discloses a security system for a cable distribution network. The system descrambles the content in the program data (column 3 lines 49-57) using a first key. The system then re-scrambles the code word with a local key (column 3 line 57 to column 4 line 10; the second key disclosed by Son carries out the function of the local key). The program data is then multiplexed and retransmitted in the future to a subscriber (column 4 lines 11-16).

Although Son discloses a system that uses a local key to re-scramble the contents in the program data, Son does not expressly disclose the remote server receiving a multiplexed signal to retrieve a code word. Son also does not expressly disclose how the code word is inserted into the program data during the multiplexing process.

However, Wasilewski discloses a method to derive the code word needed to acquire the key for descramble content in the program data (step 343 of Fig. 3). In addition, Wasilewski discloses the method of multiplexing to insert the code word into the program data (Fig. 3 part 321). Wasilewski discloses the key being contained in the EMM and therefore inserted into the

EMM (page 4 paragraph 0070). The EMM is then sent to the user, therefore allowing access to the client (page 5 paragraph 0076).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the methods of Wasilewski to send the data from the broadcast source in Son in a multiplexed form as in Wasilewski, which acquire the codeword and decrypt the data as in Son. The information is re-encrypted as in Son and the codeword is inserted into the program data using the multiplexing process disclosed in the system by Wasilewski. One of ordinary skill in the art would have been motivated to do this because service organizations require access restrictions that are both more secure and more flexible than those in conventional systems, so as to prevent illegal reproductions of the program data while providing legal users a simple and elegant method of viewing the program data.

*In reference to claims 5 and 11*, further comprising inserting modified access criteria in addition to the re-scrambled code word (Son, column 2 lines 40-55). Since the distribution center redistributes the program data, it would be required to change the access information to facilitate access by the subscriber.

*In reference to claims 6, 12, and 19*, further comprising prior to inserting the local key the method encrypts the local key with a unit key and inserting the encrypted key into the program data for future access. Son does not expressly disclose the method of inserting the local key into the program data. Wasilewski discusses service instance encryption techniques (Wasilewski, Fig. 2A Part 204, in combination with page 5 paragraph 0076).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the key into the program data for future access as in Wasilewski in the

Art Unit: 2135

system of Son. One of ordinary skill in the art would have been motivated to do this because it would provide increased security.

*In reference to claims 7 and 13* the local key is a locally generated random number (Son, column 3 line 60 to column 4 line 10).

*In reference to claims 8, 16, and 30*, wherein the process, once initialized, is performed essentially without CPU intervention (Son, column 48-58). Since the program data is re-encrypted and stored, the CPU does not need to carry out encryption once more and is therefore not required for the multiplexing and transmission of the data.

*In reference to claims 9 and 14*, wherein the inserting of the local key comprising erasing data related to a prior key within the entitlement management message; and substituting the local key for the erased key with the entitlement management message.

Son does not expressly disclose the method of inserting the local key into the program data.

Wasilewski discloses inserting a key into the entitlement management message (Wasilewski Fig. 3 part 315). The action of erasing the data related to a prior key creates the same result as using a new key, by making the prior key unavailable for use by the client.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to encrypt the key into the program data for future access as in Wasilewski in the system of Son. One of ordinary skill in the art would have been motivated to do this because it would provide increased security.

*In reference to claims 20 and 28*, Son does not expressly disclose the method of inserting the local key into the program data. Wasilewski discloses deriving the key from the entitlement management message (Wasilewski Fig. 3 part 343).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to derive the key from the entitlement management message as in Wasilewski in the system of Son. One of ordinary skill in the art would have been motivated to do this because separating the key into two forms of delivery increases the security therefore the EMM is used as the second packet used to deliver the key.

*In reference to claims 18, 22, 26, 31, and 33*, the system disclosed by Son re-encrypts the data and then sends the data to the new subscriber. Therefore the data in the entitlement management message and the entitlement control message as received from the broadcast source, will be deleted and the new data sent to the subscriber by the remote server would be created.

*In reference to claim 24*, wherein identifying the packet with the entitlement control message comprises sorting the program data according to packet identifiers. Wasilewski discloses ECM packet identifiers that are used to identify ECM packets and therefore sort them out from the other packets (page 20 paragraph 304).

### ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2135

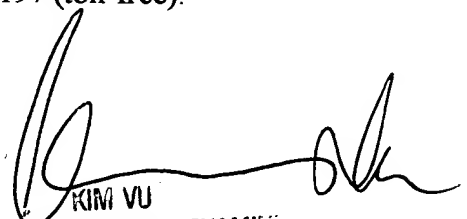
A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100